

BUNDESREPUBLIK DEUTSCHLAND

item II

EP99/07012

EJU

EPO - DG 1

09. 11. 1999

(74)



## Bescheinigung

REC'D 17 NOV 1999

WIPO PCT

Die Philips Corporate Intellectual Property GmbH in Hamburg/Deutschland hat eine  
Patentanmeldung unter der Bezeichnung

"Verschlüsselungsverfahren zum Ausführen von  
kryptographischen Operationen"

am 5. August 1999 beim Deutschen Patent- und Markenamt eingereicht und erklärt,  
daß sie dafür die Innere Priorität der Anmeldung in der Bundesrepublik Deutschland  
vom 30. September 1998, Aktenzeichen 198 45 095.8 in Anspruch nimmt.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen  
Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole  
H 04 L und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 20. Oktober 1999

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

PRIORITY  
DOCUMENTSUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

Keller

Aktenzeichen: 199 36 918.6

## Beschreibung

### Verschlüsselungsverfahren zum Ausführen von kryptographischen Operationen

5

#### Technisches Gebiet

Die Erfindung betrifft ein Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation  $y_i = f_i(x_i, k_i)$  von digital als Datenbit-

10 bzw. jeweilige Zwischenergebnisse  $y_i$  digital als Datenbitworte abgespeichert bzw. zwischengespeichert werden, gemäß dem Oberbegriff des Anspruchs 1. Die Erfindung betrifft ferner eine Verschlüsselungsvorrichtung mit einer Berechnungseinheit und Registern  $R_i$ , wobei die Berechnungseinheit wenigstens eine kryptographische Teiloperation  $y_i = f_i(x_i, k_i)$  von di-

15 gital in den Registern  $R_i$  der Verschlüsselungsvorrichtung als Datenbitworte gespeicherten Operanden  $x_i, k_i$  ausführt und das jeweilige Ergebnis bzw. Zwischenergebnisse  $y_i$  digital in den Registern  $R_i$  der Verschlüsselungsvorrichtung als Datenbitworte abspeichert bzw. zwischenspeichert, gemäß dem Oberbegriff des Anspruchs 8.

20

#### Stand der Technik

In vielen Datenverarbeitungsgeräten dienen kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem Gerät transportierten Daten. Die hierfür notwendigen Berechnungsopera-

25 tionen werden dabei sowohl von Standard-Rechenwerken als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten. Bei derartigen kryptographischen Berechnungen, wie in Fig. 1 veranschaulicht, ist es oftmals notwendig, entsprechende Speicherbereiche bzw. Register des Datenverar-

30 beitungsgerätes mit Operanden  $x_i, k_i$  zu initialisieren. Während der  $i$ -ten

Berechnung werden ggf. Zwischenergebnisse  $y_i$  in Speicherbereichen oder Registern  $R_i$  abgelegt oder abschließend das Ergebnis der Berechnung zur Weiterverarbeitung in Speicherbereichen oder Registern abgelegt. Das Register  $r_i$  befindet sich zwischen einer vorherigen  $i$ -ten kryptographischen Berechnung und einer nachfolgenden  $(i+1)$ -ten kryptographischen Berechnung. Bei den in diesem Zusammenhang verwendeten Daten  $x_i$ ,  $k_i$  bzw. Zwischenergebnissen  $y_i$  handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

Zur Berechnung der kryptographischen Algorithmen werden in den Datenverarbeitungsgeräten logische Verknüpfungen zwischen Operanden  $k_i$  bzw. Zwischenergebnissen  $y_i$  bzw.  $x_i$ ,  $x_{i+1}$  durchgeführt. In Abhängigkeit von der verwendeten Technologie führen diese Operationen, insbesondere das Laden der Speicherbereiche bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert einer Bit-Speicherzelle geändert wird, d.h. sein Wert sich von "0" auf "1" bzw. von "1" auf "0" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers einen Stromverbrauch proportional zum Hamminggewicht des Operanden (=Anzahl der Bits mit dem Wert "1") bzw. der Differenz im Hamminggewicht ansteigen. Durch eine entspre-

chende Analyse dieser Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln, möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnten beispielsweise bei sehr kleinen Signaländerungen eine hinreichende Extraktion der Informa-

tionen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte Kryptoanalyse der kryptographischen Operationen, Algorithmen, Operanden bzw. Daten erfolgreich ausführen kann.

Aus der US 5 297 201 ist es bekannt, einen Hochfrequenz abstrahlenden Computer mit einer Einrichtung zu kombinieren, welche ebenfalls Hochfrequenz ähnlich zu derjenigen des Computers abstrahlt. Dadurch ist es für einen unberechtigten Dritten nicht mehr möglich, die Hochfrequenzabstrahlung des Computers zu dekodieren. Eine Kryptoanalyse durch einen Dritten, der unmittelbar Zugang zum Computer hat, kann dieses System jedoch nicht verhindern.

Um bei Chipkarten eine Korrelation zwischen einer Ausgabe eines Ergebnisses einer kryptographischen Operation bzw. einer Übertragung einer Schlüsselinformation für eine kryptographischen Operation und der kryptographischen Operation selbst zu beseitigen ist es aus Patent Abstracts of Japan 10069222A bekannt, das Ergebnis der kryptographischen Operation bzw. die Übertragung der Schlüsselinformation für die kryptographischen Operationen zeitlich zu verzögern. Jedoch ist auch dieses System mittels der "Differential Power Analysis" analysierbar, da sich auch die verzögerte Datenübertragung im Stromverbrauch des Datenverarbeitungsgerätes verrät.

#### Darstellung der Erfindung, Aufgabe, Lösung, Vorteile

Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren sowie eine verbesserte Vorrichtung der obengenannten Art zur Verfügung

zu stellen, welche die obengenannten Nachteile beseitigen und eine erfolgreiche Kryptoanalyse mittels Beobachtung eines Stromverbrauches eines Datenverarbeitungsgerätes wirksam verhindert.

- 5 Diese Aufgabe wird durch ein Verfahren der o.g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen gelöst.

10 Dazu ist es erfindungsgemäß vorgesehen, dass wenigstens eines der Daten  $x_i$ ,  $k_i$  und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis  $y_i$  in Abhängigkeit von einem auf Zufallszahlen basierenden Steuersignal  $r_i$  wahlweise bitweise zu  $\bar{y} = f(x_i)$  und/oder  $\bar{y}_i$  komplementiert wird oder nicht.

15 Dies hat den Vorteil, dass bei wiederholter Ausführung derselben kryptographischen Operation andere Bitfolgen bearbeitet bzw. abgespeichert werden, so dass sich bei der jeweiligen Ausführung einer kryptographischen Operation bzw. mehrerer kryptographischer Operationen andere Stromänderungen des Datenverarbeitungsgerätes ergeben. Unabhängig vom eigentlichen Wert der Teilergebnisse wird somit bei wiederholter Ausführung der Gesamtberechnung erreicht, dass jeder Datenpfad bei  
20 einer echten Zufallszahlenreihe gleichhäufig bzw. bei einer Pseudozufallszahlenreihe nahezu gleichhäufig von "0" auf "0", von "0" auf "1", von "1" auf "0" und von "1" auf "1" wechselt. Da jedoch das auf Zufallszahlen basierende Steuersignal  $r_i$  nicht bekannt bzw. vorbestimmt ist, fehlt eine Korrelation zwischen den Stromänderungen und den Bitwerten der Daten und

- 25 Ergebnisse, so dass eine "Differential Power Analysis" nicht mehr zu einer erfolgreichen Kryptoanalyse führt. Mit anderen Worten enthält der mittlere Stromverbrauch der Gesamtoperation keine brauchbare Information über die verwendeten Teiloperanden bzw. Zwischenergebnisse in den Teiloperationen.

Vorzugsweise Weitergestaltungen der Vorrichtung sind in den Ansprüchen 2 bis 7 beschrieben.

5 Zweckmäßigerweise werden in den kryptographischen Teiloperationen eine oder mehrere XOR-Verknüpfungen (Exklusiv-Oder-Verknüpfung) ausgeführt.

10 Die Daten umfassen beispielsweise kryptographische Schlüssel und/oder Operanden.

In einer bevorzugten Ausführungsform werden Zwischenergebnisse  $y_i$  zwischen der Ausführung von aufeinander folgenden kryptographischen Teiloperationen in einem Register  $R_i$  zwischengespeichert und als Operand  $x_{i+1}$  der nachfolgenden kryptographischen Teiloperationen zugeführt.

20 Zum Herstellen eines originalen, nicht invertierten Wertes nach jeder Teiloperation wird eine aus dem Zwischenergebnis  $y_i$  einer vorangegangenen Teiloperation  $i$  erhaltene Bitfolge  $x_{i+1} = y_i$  für eine nachfolgende Teiloperation  $i+1$  bitweise zu  $\bar{x}_{i+1}$  komplementiert, wenn die Daten  $x_i$ ,  $k_i$  der vorangegangenen Teiloperation  $i$  bitweise komplementiert wurden.

In einer besonders bevorzugten Ausführungsform werden bei der bitweisen Komplementierung wenigstens ein Bitwert, insbesondere die geraden Bitwerte, die ungeraden Bitwerte oder alle Bitwerte, eines Datenbitwortes  $x_i$ ,  $k_i$ , bzw.  $y_i$  invertiert. Hierbei ist es besonders vorteilhaft, wenn eine Invertierung von Bitwerten bzw. Bitadressen eines Datenbitwortes  $x_i$ ,  $k_i$ , bzw.  $y_i$  bei der bitweisen Komplementierung mittels einer XOR-Operation (Exklusiv-Oder-Operation) durchgeführt wird.

Bei einer Vorrichtung der o.g. Art ist erfindungsgemäß wenigstens ein von einem Steuersignal  $r_i$  steuerbarer Inverter für wenigstens eines der Daten  $x_i$ ,  $k_i$  und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis  $y_i$ , ein Zufallszahlengenerator, welcher Zufallszahlen erzeugt, sowie eine Vorrichtung zum Erzeugen des Steuersignals  $r_i$  auf den Zufallszahlen basierend vorgesehen, wobei der steuerbare Inverter in Abhängigkeit von dem Steuersignal  $r_i$  wahlweise die Bitfolgen  $x_i$ ,  $k_i$  bzw.  $y_i$  zu ihrem bitweisen Komplement  $\bar{x}_i$ ,  $\bar{k}_i$  bzw.  $\bar{y}_i$  umsetzt oder unverändert lässt.

10

Dies hat den Vorteil, dass bei wiederholter Ausführung derselben kryptographischen Operation andere Bitfolgen bearbeitet bzw. abgespeichert werden, so dass sich bei der jeweiligen Ausführung der kryptographischen Operation bzw. kryptographischen Operationen andere Stromänderungen des Datenverarbeitungsgerätes ergeben. Unabhängig vom eigentlichen Wert der Teilergebnisse wird somit bei wiederholter Ausführung der Gesamtberechnung erreicht, dass jeder Datenpfad bei einer echten Zufallszahlenreihe gleichhäufig bzw. bei einer Pseudozufallszahlenreihe nahezu gleichhäufig von "0" auf "0", von "0" auf "1", von "1" auf "0" und von "1" auf "1" wechselt. Da jedoch das auf Zufallszahlen basierende Steuersignal  $r_i$  nicht bekannt bzw. vorbestimmt ist, fehlt eine Korrelation zwischen den Stromänderungen und den Bitwerten der Daten und Ergebnisse, so dass eine "Differential Power Analysis" nicht mehr zu einer erfolgreichen Kryptoanalyse führt. Mit anderen Worten enthält der mittlere Stromver-

25

brauch der Gesamtoperation keine brauchbare Information über die verwendeten Teiloperanden bzw. Zwischenergebnisse in den Teiloperationen.

Vorzugsweise Weitergestaltungen der Vorrichtung sind in den Ansprüchen 9 bis 14 beschrieben.

5 In einer bevorzugten Ausführungsform ist wenigstens einem Register  $R_i$  ein Inverter nachgeschaltet, welcher das identische Steuersignal  $r_i$  erhält, wie die der  $i$ -ten Teiloperation vorgeschalteten Inverter für die Daten  $x_i$ ,  $k_i$ . Dieser einem Register  $R_i$  der  $i$ -ten Teiloperation nachgeschaltete Inverter ist dabei bevorzugt mit einem der nachfolgenden  $(i+1)$ -ten Teiloperation vorgeschalteten Inverter für ein Eingangsdatum  $x_{i+1}$  kombiniert. Der kombinierte Inverter erhält zweckmäßigerweise sowohl das Steuersignal  $r_i$  der vorangegangenen  $i$ -ten Teiloperation als auch das Steuersignal  $r_{i+1}$  der nachfolgenden  $(i+1)$ -ten Teiloperation.

15 Die Daten umfassen beispielsweise kryptographische Schlüssel und/oder Operanden.

20 In einer bevorzugten Ausführungsform speichert ein Register  $R_i$  zwischen einer vorangegangenen  $i$ -ten Teiloperation und einer nachfolgenden  $(i+1)$ -ten Teiloperation ein Zwischenergebnis  $y_i$  der vorangegangenen  $i$ -ten Teiloperation und leitet dieses Zwischenergebnis als Eingangswert  $x_{i+1}$  an die nachfolgende  $(i+1)$ -te Teiloperation weiter.

Zweckmäßigerweise invertiert die bitweise Komplementierung wenigstens einen Bitwert, insbesondere die geraden Bitwerte, die ungeraden Bitwerte oder alle Bitwerte, eines Datenbitwortes  $x_i$ ,  $k_i$ , bzw.  $y_i$ .

#### Kurze Beschreibung der Zeichnungen

Nachstehend wird die Erfindung anhand der beigefügten Zeichnungen näher erläutert. Diese zeigen in



Fig. 1 ein Ablaufschema eines Teiles einer kryptographischen Operation gemäß dem Stand der Technik,

Fig. 2 ein Ablaufschema eines Teiles einer ersten bevorzugten Ausführungsform einer erfindungsgemäßen kryptographischen Operation und

Fig. 3 ein Ablaufschema eines Teiles einer zweiten bevorzugten Ausführungsform einer erfindungsgemäßen kryptographischen Operation.

#### Bester Weg zur Ausführung der Erfindung

Bei der in Fig. 2 dargestellten ersten bevorzugten Ausführungsform eines erfindungsgemäßen Verschlüsselungsverfahrens wird durch eine Kette von Teiloperationen  $f_i(x_i, k_i)$ , innerhalb derer ein oder mehrere logische XOR-Verknüpfungen (Exklusiv-Oder-Verknüpfung) ausgeführt werden, eine kryptographische Gesamtoperation durchgeführt. Dargestellt sind zwei Teiloperationen, nämlich die  $i$ -te Teiloperation 10 und die  $(i+1)$ -te Teiloperation 12, wobei jede Teiloperation von einer Berechnungseinheit ausgeführt wird. Jeder Teiloperation 10, 12 ist eine Speicherzelle oder ein Register  $R_i$  14 bzw. eine Speicherzelle oder ein Register  $R_{i+1}$  16 nachgeschaltet. Jede Teiloperation 10, 12 hat als Eingangswert ein Datum  $x_i, x_{i+1}$  sowie einen Operanden  $k_i, k_{i+1}$ , welche als Datenbitworte zur Verfügung stehen.

25

Jeder Teiloperation 10, 12 vorgeschaltet ist jeweils ein steuerbarer Inverter 18 bzw. 20 für die Daten  $x_i, x_{i+1}$  sowie jeweils ein steuerbarer Inverter 22, 24 für die Operanden  $k_i, k_{i+1}$ . Ferner ist bei jeder Teiloperation 10, 12 dem jeweiligen Register  $R_i$  14 bzw.  $R_{i+1}$  16 ein steuerbarer Inverter 26, 28 für das Zwischenergebnis  $y_i, y_{i+1}$  nachgeschaltet, wobei dieses Zwischen-

30

ergebnis von dem jeweiligen Register  $R_i$  14 bzw.  $R_{i+1}$  16 als Eingangsdaten  $x_{i+1}$  bzw.  $x_{i+2}$  an eine nachfolgende Teiloperation 12 weiter gegeben werden. Diese Inverter 18 bis 28 sind durch ein Steuersignal  $r_i$  bzw.  $r_{i+1}$  derart steuerbar, dass sie in Abhängigkeit von dem jeweiligen Steuersignal  $r_i$  bzw.  $r_{i+1}$  wahlweise die zugeordneten Datenbitworte bitweise komplementieren oder nicht. Hierbei erhalten alle Inverter 18, 22, 26 bzw. 20, 24, 28 einer Teiloperation 10 bzw. 12 dasselbe Steuersignal  $r_i$  bzw.  $r_{i+1}$ . Mit anderen Worten wird die Entscheidung, ob eine Invertierung der entsprechenden Eingangswerte der Inverter 18 bis 28 durchgeführt wird oder ob die Eingangswerte unbearbeitet die Inverter 18 bis 28 durchlaufen, durch das zusätzliche Steuersignal  $r_i$  bzw.  $r_{i+1}$  entschieden. Diese Anordnung von Registern 14, 16 zwischen Teiloperationen 10, 12 findet vor allem dann Anwendung, wenn die Teiloperationen 10, 12 zeitlich nacheinander von ein und derselben Einheit berechnet werden und somit die Teilergebnisse zwischengespeichert werden müssen.

Das Steuersignal wird durch Zufallswerte aus einem Zufallsgenerator dahingehend gesteuert, dass die Teiloperation abhängig vom Wert der Zufallszahlen entweder das Originalergebnis  $y = f(x, k)$  oder das bitinvertierte Ergebnis  $\bar{y} = f(\bar{x}, \bar{k})$  liefert. Hierdurch wird realisiert, dass sowohl die Berechnung als auch die Speicherung der Daten in den Registern  $R_i$  14, 18 entweder mit Originalwerten oder mit bitinvertierten Werten durchgeführt wird. Unabhängig vom eigentlichen Wert der Teilergebnisse wird somit bei wiederholter Ausführung der Gesamtberechnung erreicht, dass jeder Datenpfad gleich häufig von "0" auf "0", von "0" auf "1", von "1" auf "0" und von "1" auf "1" wechselt. Der mittlere Stromverbrauch der Gesamtoperation enthält somit keine brauchbare Information über die verwendeten Teiloperanden  $k_i$  bzw. Zwischenergebnisse  $y_i$  in den Teiloperationen 10, 12. Der dem Register 14, 16 nachgeschaltete Inverter 26, 28

stellt für die folgende Teiloperation 12 wieder den originalen, nicht invertierten Wert her.

5 Die zweite bevorzugte Ausführungsform des erfindungsgemäßen Verschlüsselungsverfahrens gemäß Fig. 3 entspricht der ersten Ausführungsform von Fig. 2 mit dem einzigen Unterschied, dass die den Registern 14, 16 nachgeschalteten Inverter 26, 28 mit dem jeweiligen Eingangsinverter 20 der folgenden Stufe 12 zu einem Inverter 30 kombiniert sind.

10

Die Inverter invertieren beispielsweise auch nur einen Teil der Bitwerte des jeweiligen Datenbitwortes. So werden beispielsweise nur die geraden oder ungeraden Bitwerte bzw. Bitadressen invertiert. Die Invertierung der Bitwerte erfolgt beispielsweise mittels einer XOR-Operation (Exklusiv-  
15 Oder-Operation).

---

### Patentansprüche

5

1. Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation  $y_i = f_i(x_i, k_i)$  von digital als Datenbitworte gespeicherten Daten  $x_i$ ,  $k_i$  ausgeführt und das jeweilige Ergebnis bzw. jeweilige Zwischenergebnisse  $y_i$  digital als Datenbitworte abgespeichert bzw. zwischengespeichert werden, dadurch gekennzeichnet, dass

10

wenigstens eines der Daten  $x_i$ ,  $k_i$  und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis  $y_i$  in Abhängigkeit von einem auf Zufallszahlen basierenden Steuersignal  $r_i$  wahlweise bitweise zu  $\bar{x}_i$ ,  $\bar{k}_i$  und/oder  $\bar{y}_i$  komplementiert wird oder nicht.

15

2. Verschlüsselungsverfahren nach Anspruch 1, dadurch gekennzeichnet, dass in den kryptographischen Teiloperationen eine oder mehrere XOR-Verknüpfungen (Exklusiv-Oder-Verknüpfung) ausgeführt werden.

20

3. Verschlüsselungsverfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Daten kryptographische Schlüssel und/oder Operanden umfassen.

25

4. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass

Zwischenergebnisse  $y_i$  zwischen der Ausführung von aufeinander folgenden kryptographischen Teiloperationen in einem Register  $R_i$  zwischengespeichert und als Operand  $x_{i+1}$  der nachfolgenden kryptographischen Teiloperationen zugeführt werden.

5

5. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet, dass

10

eine aus dem Zwischenergebnis  $y_i$  einer vorangegangenen Teiloperation  $i$  erhaltene Bitfolge  $x_{i+1} = y_i$  für eine nachfolgende Teiloperation  $i+1$  bitweise zu  $\bar{x}_{i+1}$  komplementiert wird, wenn die Daten  $x_i$ ,  $k_i$  der vorangegangenen Teiloperation  $i$  bitweise komplementiert wurden.

15

6. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet, dass

bei der bitweisen Komplementierung wenigstens ein Bitwert, insbesondere die geraden Bitwerte, die ungeraden Bitwerte oder alle Bitwerte, eines Datenbitwortes  $x_i$ ,  $k_i$ , bzw.  $y_i$  invertiert werden.

20

7. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche,

dadurch gekennzeichnet, dass

25

eine Invertierung von Bitwerten bzw. Bitadressen eines Datenbitwortes  $x_i$ ,  $k_i$ , bzw.  $y_i$  bei der bitweisen Komplementierung mittels einer XOR-Operation (Exklusiv-Oder-Operation) durchgeführt wird.

8. Verschlüsselungsvorrichtung mit einer Berechnungseinheit und Registern  $R_i$  (14, 16), wobei die Berechnungseinheit wenigstens eine kryptographische Teiloperation  $y_i = f_i(x_i, k_i)$  (10, 12) von digital in den Registern  $R_i$  (14, 16) der Verschlüsselungsvorrichtung als Datenbitworte gespeicherten Operanden  $x_i, k_i$  ausführt und das jeweilige Ergebnis bzw. Zwischenergebnisse  $y_i$  digital in den Registern  $R_i$  (14, 16) der Verschlüsselungsvorrichtung als Datenbitworte abspeichert bzw. zwischenspeichert, dadurch gekennzeichnet, dass
- 10 wenigstens ein von einem Steuersignal  $r_i$  steuerbarer Inverter (18 bis 28; 30) für wenigstens eines der Daten  $x_i, k_i$  und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis  $y_i$ , ein Zufallszahlengenerator, welcher Zufallszahlen erzeugt, sowie eine Vorrichtung zum Erzeugen des Steuersignals  $r_i$  auf den Zufallszahlen basierend
- 15 vorgesehen ist, wobei der steuerbare Inverter (18 bis 28; 30) in Abhängigkeit von dem Steuersignals  $r_i$  wahlweise die Bitfolgen  $x_i, k_i$  bzw.  $y_i$  zu ihrem bitweisen Komplement  $\bar{x}_i, \bar{k}_i$  bzw.  $\bar{y}_i$  umsetzt oder unverändert lässt.
- 20 9. Verschlüsselungsvorrichtung nach Anspruch 8, dadurch gekennzeichnet, dass
- wenigstens einem Register  $R_i$  (14, 16) ein Inverter (26, 28; 30) nachgeschaltet ist, welcher das identische Steuersignal  $r_i$  erhält, wie die der  $i$ -ten Teiloperation (10, 12) vorgeschalteten Inverter
- 
- 25 (18, 20) für die Daten  $x_i, k_i$ .
10. Verschlüsselungsvorrichtung nach Anspruch 9, dadurch gekennzeichnet, dass

der einem Register  $R_i$  (14, 16) der  $i$ -ten Teiloperation (10, 12) nachgeschaltete Inverter (26, 28) mit einem der nachfolgenden  $(i+1)$ -ten Teiloperation (12) vorgeschalteten Inverter (20) für ein Eingangsdatum  $x_{i+1}$  kombiniert ist.

5

11. Verschlüsselungsvorrichtung nach Anspruch 10, dadurch gekennzeichnet, dass der kombinierte Inverter (30) sowohl das Steuersignal  $r_i$  der vorangegangenen  $i$ -ten Teiloperation (10) als auch das Steuersignal  $r_{i+1}$  der nachfolgenden  $(i+1)$ -ten Teiloperation (12) erhält.

10

12. Verschlüsselungsvorrichtung nach einem der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass die Daten kryptographische Schlüssel und/oder Operanden umfassen.

15

13. Verschlüsselungsvorrichtung nach einem der Ansprüche 8 bis 12, dadurch gekennzeichnet, dass ein Register  $R_i$  (14, 16) zwischen einer vorangegangenen  $i$ -ten Teiloperation (10) und einer nachfolgenden  $(i+1)$ -ten Teiloperation (12) ein Zwischenergebnis  $y_i$  der vorangegangenen  $i$ -ten Teiloperation (10) speichert und dieses Zwischenergebnis als Eingangswert  $x_{i+1}$  an die nachfolgende  $(i+1)$ -te Teiloperation (12) weiterleitet.

20

- 
- 25 14. Verschlüsselungsvorrichtung nach einem der Ansprüche 8 bis 13, dadurch gekennzeichnet, dass die bitweise Komplementierung wenigstens einen Bitwert, insbesondere die geraden Bitwerte, die ungeraden Bitwerte oder alle Bitwerte, eines Datenbitwortes  $x_i$ ,  $k_i$ , bzw.  $y_i$  invertiert.

BEZUGSZEICHENLISTE

	10	i-te Teiloperation
5	12	(i+1)-te Teiloperation
	14	Register $R_i$
	16	Register $R_{i+1}$
	18	steuerbarer Inverter für $x_i$
	20	steuerbarer Inverter für $x_{i+1}$
10	22	steuerbarer Inverter für $k_i$
	24	steuerbarer Inverter für $k_{i+1}$
	26	steuerbarer Inverter für $y_i$
	28	steuerbarer Inverter für $y_{i+1}$
	30	kombinierter Inverter

---



Fig.1

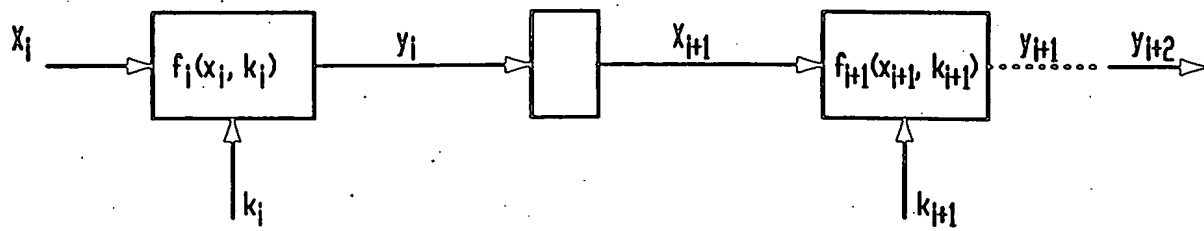


Fig.2

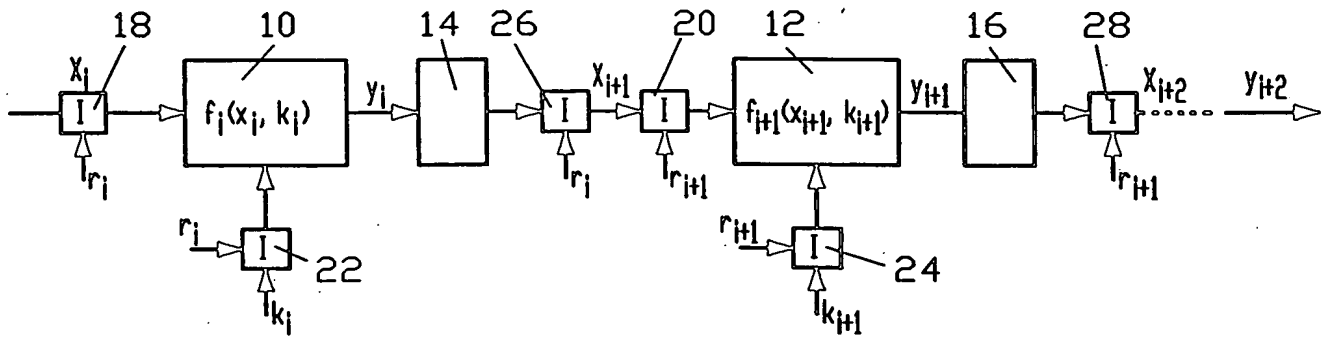
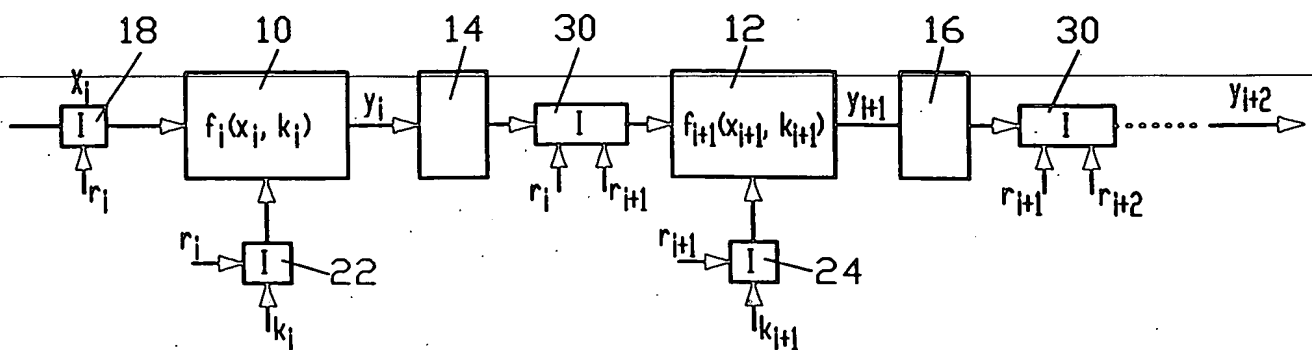


Fig.3



### Zusammenfassung

Die vorliegende Erfindung betrifft ein Verschlüsselungsverfahren sowie eine Verschlüsselungsvorrichtung, wobei wenigstens eine kryptographische Teiloperation  $y_i = f_i(x_i, k_i)$  von digital als Datenbitworte gespeicherten Daten  $x_i, k_i$  ausgeführt und das jeweilige Ergebnis bzw. jeweilige Zwischenergebnisse  $y_i$  digital als Datenbitworte abgespeichert bzw. zwischengespeichert werden. Hierbei wird wenigstens eines der Daten  $x_i, k_i$  und/oder das Ergebnis bzw. wenigstens ein Zwischenergebnis  $y_i$  in Abhängigkeit von einem auf Zufallszahlen basierenden Steuersignal  $r_i$  wahlweise bitweise zu  $\bar{x}_i, \bar{k}_i$  und/oder  $\bar{y}_i$  komplementiert oder nicht. (Fig. 2)